

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 09/898,310
Applicants : Teng Pin Poo and Lay Chuan Lim
Filed : July 3, 2001
Art Unit : 2137
Examiner : Gelagay, Shewaye
Confirm. No. : 2223

Docket No. : 1601457-0008
Customer No. : 007470

Mail Stop **Appeal Brief – Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission

I hereby certify that this paper is being transmitted to the U.S. Patent and Trademark Office via the Electronic Filing System in accordance with 37 C.F.R. § 1.6(a)(4) on the date indicated below.

Date: August 29, 2008

By: Gail A. Ohlsson
Gail A. Ohlsson

APPEAL BRIEF

This is an appeal pursuant to 37 C.F.R. § 41.37 from the decision of the Examiner in the above-identified application as set forth in the final Office Action dated July 10, 2007. The rejected claims are reproduced in Appendix A. A Notice of Appeal and a Pre-Appeal Brief Request for Review were filed on January 10, 2008. A Notice of Panel Decision from Pre-Appeal Brief Review stating that the application remains under appeal was mailed on February 29, 2008.

The fee of \$510.00 for filing an Appeal Brief (Large Entity) pursuant to 37 C.F.R. § 41.20(b)(2) is enclosed herewith. A Petition for a five-month extension of time is enclosed herewith along with the fee of \$2,230.00 (Large Entity). Any additional fees or

charges in connection with this application may be charged to White & Case Deposit Account No. 50-3672.

REAL PARTY IN INTEREST

The assignee, Trek Technology (Singapore) Pte. Ltd., of applicant(s), Teng Pin Poo and Lay Chuan Lim, is the real party of interest in the above-identified U.S. Patent Application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals and/or interferences related to the above-identified application at the present time.

STATUS OF CLAIMS

Claims 1-27 have been rejected. Claims 1-27 are on appeal.

STATUS OF AMENDMENTS

Appellants amended certain of claims 1-21 and added new claims 22-27 in an Amendment dated April 30, 2007. These amendments were entered and claims 1-27 were rejected in the final Office Action dated July 10, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claims 1 and 11

Appellant's invention is directed to a biometrics-based access control device having biometrics-based authentication capabilities so the device can authenticate users before granting access to a restricted resource. As illustrated in Figure 1B and Figure 2 of the application, reproduced below, portable device 170 has a housing, within which is housed a microprocessor 111, a biometrics-based authentication module 150 controlled by the microprocessor 111, a non-volatile memory 117, a memory controller 133, and a

the device. Non-volatile memory 117 stores firmware such as firmware 117a for reading fingerprint sensor 152, firmware 117b for processing fingerprint images, firmware 117c for generating templates, firmware 117d for encrypting fingerprint images and/or templates, and firmware 117e for verifying fingerprint authenticity. *See* Specification page 8, lines 30-33. Upon its first use, portable device 170 guides the user through the registration process wherein the user places his or her finger on fingerprint sensor 152, located on the surface of portable device 170, and sensor 152 is read to capture an acceptable image of the fingerprint. *See* Specification page 12, lines 1-10. An encrypted template is generated based on the fingerprint image and stored into non-volatile memory 117. *See* Specification page 12, lines 13-17. During the authentication process, another image of the user's fingerprint is taken when the user places his or her finger on sensor 152. *See* Specification page 12, lines 32 through page 13, line 1. Microprocessor 111 directs the retrieval of the registered fingerprint template from non-volatile memory 117. *See* Specification page 13, lines 9-10. Next, verification module 117e compares the recently taken fingerprint image against the registered image. *See* Specification page 13, lines 15-17. If a match is detected, the user is authenticated and granted access to the restricted resource. If no match is detected, access to the restricted resource is denied. *See* Specification page 14, line 24 – page 15, line 15. Examples of restricted resources are files or programs on a host platform, secured locations such as hotel rooms and bank vaults, and machinery that requires proper training for operation. *Id.*

In embodiments where the portable device is also used as a secure storage device, if a match is detected the user is authenticated and granted access to the portable device.

See Specification page 14, lines 6-10. If no match is detected, such access is denied. *See* Specification page 13, lines 22-23.

Independent Claim 17

Appellants' invention is directed to a biometrics-based access control method implemented using a portable device 70 that has a non-volatile memory 117 with a minimum of 8 MB of capacity. *See* Specification page 5, lines 22-24. Portable device 70 is directly plugged into a USB socket communicatively coupled to a restricted resource. *See* Specification page 11, lines 5-9; page 14, line 24 – page 15, line 15. A first biometrics marker, such as a fingerprint, is obtained from a user with a biometrics sensor 52 installed on the portable device 70. *See* Specification page 12, line 32 – page 13, line 1; FIG. 10, step 230. Then a registered biometrics marker is retrieved from a flash memory 20 of the portable device 70. *See* Specification page 13, lines 7-10; FIG. 10, step 240. The registered biometrics marker was previously stored in the flash memory 20 during a registration process. *See* Specification page 12, lines 1-31; FIG. 10, steps 225-255. The first biometrics marker is compared to the registered biometrics marker, and the user's access to the restricted resource is denied if the first biometrics marker does not match the registered biometrics marker. *See* Specification page 13, lines 14-17; FIG. 10, step 260. If the first biometrics marker matches the registered biometrics marker, an authentication success is signaled and access to the restricted resource is granted. *See* Specification page 13, lines 14-17, FIG. 10, steps 260 and 280. Examples of restricted resources are files or programs on a host platform, secured locations such as hotel rooms and bank vaults, and machinery that requires proper training for operation. *See* Specification page 14, line 24 – page 15, line 15.

GROUND OF REJECTION TO BE REVIEWED

1. The rejection of claims 1, 2, 4, 5, 7, 8, 11, 12, 14, 15, 17, 18, 20, 23, 25, and 27 as unpatentable under 35 U.S.C. § 103(a) over U.S. Patent No. 6,671,808 to Abbott et al. (“Abbott”) in view of U.S. Patent No. 7,036,738 to Vanzini et al. (“Vanzini”).
2. The rejection of claims 3 and 13 as unpatentable under 35 U.S.C. § 103(a) over Abbott in view of Vanzini and further in view of U.S. Patent Application Publication No. 2002/0145507 to Foster.
3. The rejection of claims 6, 16, and 21 as unpatentable under 35 U.S.C. §103(a) over Abbott in view of Vanzini and further in view of U.S. Patent No. 5,815,252 to Price-Francis.
4. The rejection of claims 9 and 10 as unpatentable under 35 U.S.C. §103(a) over Abbott in view of Vanzini and further in view of U.S. Patent Application Publication No. 2001/0045458 to Polansky.
5. The rejection of claim 19 as unpatentable under 35 U.S.C. § 103(a) over Abbott in view of Vanzini and further in view of U.S. Patent No. 6,990,587 to Willins et al. (“Willins”).
6. The rejection of claims 22, 24, and 26 as unpatentable under 35 U.S.C. § 103(a) over Abbott in view of Vanzini and further in view of U.S. Patent Application Publication No. 2001/0004326 to Terasaki et al. (“Terasaki”).

ARGUMENT

1. Rejection of claims 1, 2, 4, 5, 7, 8, 11, 12, 14, 15, 17, 18, 20, 23, 25, and 27

The Examiner rejected claims 1, 2, 4, 5, 7, 8, 11, 12, 14, 15, 17, 18, 20, 23, 25, and 27 under 35 U.S.C. § 103(a) as being unpatentable over Abbott in view of Vanzini. Appellants respectfully traverse.

Independent claims 1, 11, and 17

Claim 1 recites that the biometrics-based authentication module is configured to “grant access to the restricted resource provided that the biometrics-based authentication module authenticates the user’s identity” and to “grant access to the user data stored in the non-volatile memory provided that the biometrics-based authentication module authenticates the user’s identity.” In other words, the biometrics-based authentication module is capable of performing *two* functions: controlling access to a restricted resource *and* controlling access to user data stored in a non-volatile memory of the access control device. Claim 1 also recites that the non-volatile memory is capable of storing user data and has “a minimum of 8 MB of capacity.”

The Examiner cites to Abbott as disclosing these limitations, but the biometric sensor of Abbott only has *one* function: controlling access to passwords stored in the personal key. Abbott does not disclose a biometrics-based authentication module that is capable of controlling access to user data stored in a non-volatile memory having a capacity of at least 8 MB, *and* controlling access to a restricted resource.

Abbott discloses a personal key that stores a number of passwords for a single user. The purpose of the personal key is to relieve the user from the task of

remembering multiple passwords (col. 3, lines 35-38). The biometrics module of Abbott is used to authenticate the user's access to the passwords stored on the personal key, providing security for the passwords (col. 3, lines 44-48; col. 7, line 17 – col. 8, line 6). In Abbott's disclosure, the passwords stored on the personal key enable access to a restricted resource (e.g., software on a host computer). The biometrics module of Abbott unlocks the set of passwords stored on the personal key, and one of the stored passwords unlocks a restricted resource. If a user successfully gains access to the passwords on the personal key using the biometrics module, the user cannot access a restricted resource unless the personal key contains the correct password for that resource. With Abbott's personal key, a successful biometrics-based authentication only allows access to the passwords stored on the personal key.

In contrast, the device of claim 1 controls access to a restricted resource without requiring the extra step of supplying a password. The device of claim 1 includes a biometrics-based authentication module that grants access to a restricted resource if the user's identity is authenticated. No passwords are required to gain access to the restricted resource if the biometrics-based authentication is successful.

The biometrics module disclosed in Abbott only has one function: controlling access to passwords stored on the personal key. Abbott does not disclose the biometrics-based authentication module recited in claim 1 that is capable of controlling access to a restricted resource *and* controlling access to user data stored in a non-volatile memory with a minimum of 8 MB of capacity.

Even though the Examiner did not argue in the Office Action that it would have been obvious to modify the biometrics module of Abbott to control access to a

restricted resource outside of the personal key, Appellants submit that such a modification would not have been obvious. It would not have been obvious to modify the personal key of Abbott to eliminate the need for storing passwords because the whole purpose of the Abbott device is to store multiple passwords for various restricted resources. If a biometrics-based authentication is used for directly granting access to various restricted resources, storing multiple passwords as taught by Abbott would be completely unnecessary. By teaching storage of multiple passwords in a personal key where the passwords are required for access to restricted resources, Abbott teaches away from using a biometrics-based authentication module to control access to a restricted resource.

The Examiner previously acknowledged that Abbott does not disclose a non-volatile memory and a biometrics-based authentication module that is configured to grant access to the user data stored in the non-volatile memory provided that the biometrics-based authentication module authenticates the user's identity (Office Action dated 10/30/2006, pg 3). But the Examiner now mistakenly asserts that Abbott discloses this limitation, citing col. 6, line 66 – col. 7, line 16. This portion of Abbott discloses that functions of other devices, such as a paging transceiver, may be incorporated within the personal key or that the personal key can store programs and instructions such as a calendar. But Abbott does not disclose that access to a paging transceiver, programs, or instructions is controlled by the biometric sensor of the personal key. Thus Abbott does not disclose a biometrics-based authentication module configured to grant access to user data stored in a non-volatile memory that has a capacity of at least 8 MB.

The Examiner stated that Abbott does not disclose a non-volatile memory having a minimum of 8 MB of capacity, and that Vanzini does. Vanzini discloses a two-part system for storing a user's data files that includes a smart card and a card reader (col. 3, lines 55-67). A user authenticates to the smart card using a password and in turn the smart card controls access to data stored on the card reader (col. 4, lines 11-22). Vanzini's two-part system teaches away from the device of claim 1, which has a biometrics-based authentication module and a non-volatile memory housed within a single housing.

The system of Vanzini requires the user to enter a password to authenticate to the smart card (col. 6, lines 3-6). In contrast, the whole purpose of the Abbott device is to store passwords so the user does not have to enter them or even remember them. The Vanzini system requires a two-step process for obtaining access to data stored on the system: authentication of a password and then authentication of the smart card. In contrast, the personal key of Abbott requires one step of a biometrics authentication to obtain access to the passwords stored on the personal key. Thus one of ordinary skill in the art would not be motivated to combine the teachings of Vanzini with the teachings of Abbott. Further, the combination of Abbott and Vanzini does not disclose, teach or suggest all of the limitations of claim 1. Neither Abbott nor Vanzini discloses a biometrics-based authentication module capable of controlling access to user data stored in a non-volatile memory *and* controlling access to a restricted resource. Appellants respectfully submit that claim 1 is not obvious in view of the cited references and is in condition for allowance.

Claim 11 recites “a non-volatile memory . . . having a minimum of 8 MB of capacity” and “a biometrics-based authentication module . . . configured to . . . determine whether the second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise.” The Examiner cites to Abbott as disclosing the claimed biometrics-based authentication module. But as set forth above, the personal key of Abbott uses a biometrics sensor to unlock passwords stored on the personal key, and then uses one of the stored passwords to unlock a restricted resource. In contrast, the biometrics-based authentication module of claim 11 controls access to a restricted resource without requiring a password. Also as set forth above, one of ordinary skill in the art would not be motivated to combine the teachings of Vanzini with the teachings of Abbott, and such a combination does not disclose, teach, or suggest all of the limitations of claim 11. Appellants respectfully submit that claim 11 is not obvious in view of the cited references and is in condition for allowance.

Claim 17 recites a “portable device [including] . . . a memory having a minimum of 8 MB of capacity” and a step of “granting the user access to the restricted resource provided that a match is identified” by “comparing the first biometrics marker against the registered biometrics marker.” The Examiner cites to Abbott as disclosing the claimed step of granting a user access to a restricted resource provided that a first biometrics marker is matched to a registered biometrics marker. But as set forth above, the personal key of Abbott uses a biometrics sensor to unlock passwords stored on the personal key, and then uses one of the stored passwords to

unlock a restricted resource. In contrast, the method of claim 17 controls access to a restricted resource by comparing a first biometrics marker against a registered biometrics marker, without requiring a password. Also as set forth above, one of ordinary skill in the art would not be motivated to combine the teachings of Vanzini with the teachings of Abbott, and such a combination does not disclose, teach or suggest all of the limitations of claim 17. Appellants respectfully submit that claim 17 is not obvious in view of the cited references and is in condition for allowance.

Dependent claims 2, 4, 5, 7, 8, 12, 14, 15, 18, 20, 23, 25, and 27

Claims 2, 4, 5, 7, 8, 12, 14, 15, 18, 20, 23, 25, and 27 depend from one of independent claims 1, 11, and 17, and are therefore allowable for at least the same reasons.

2. Rejection of claims 3 and 13

The Examiner rejected claims 3 and 13 under 35 U.S.C. § 103(a) as unpatentable over Abbott in view of Vanzini and further in view of Foster. Appellants respectfully traverse.

Claims 3 and 13 depend from one of claims 1 and 11 and are therefore allowable for at least the same reasons. Claims 3 and 13 recite that “the biometrics-based authentication module is an iris scan authentication module.” The Examiner cites to Foster as disclosing an iris scan authentication module. Foster teaches that the biometric device can be integrated with a cell phone or a PDA. There is no teaching or suggestion in Foster that the biometric device may be part of a device that can be directly plugged into a USB socket communicatively coupled to a restricted resource. Thus one of ordinary skill in the art would not have been motivated to combine Foster

with either Abbott or Vanzini. None of the cited references, either alone or in combination, disclose, teach, or suggest all of the limitations of claims 3 and 13. Appellants respectfully submit that claims 3 and 13 are not obvious in view of the cited references and are in condition for allowance.

3. Rejection of claims 6, 16, and 21

The Examiner rejected claims 6, 16, and 21 under 35 U.S.C. §103(a) as being unpatentable over Abbott in view of Vanzini and further in view of Price-Francis. Appellants respectfully traverse.

Claims 6, 16, and 21 depend from one of claims 1, 11, and 17, and are therefore allowable for at least the same reasons. Claims 6 and 16 recite “a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module,” and claim 21 recites “providing the user with a bypass authentication procedure provided that a match is not identified.” The Examiner cites to col. 7, lines 37-47 of Price-Francis as disclosing these limitations. But the cited portion of Price-Francis discloses that other information about the card owner, such name, date of birth, height, weight, etc. can be stored on an optical card. Storing card owner information on an optical card is not a bypass mechanism for authentication when a biometrics-based authentication fails. The cited portion of Price-Francis does not teach or disclose a bypass mechanism for authentication upon determination of authentication failure by a biometrics-based authentication module. None of the cited references, either alone or in combination, disclose, teach, or suggest all of the limitations of claims 6, 16, and 21. Appellants respectfully submit that claims 6, 16, and 21 are not obvious in view of the cited references and are in condition for allowance.

4. Rejection of claims 9 and 10

The Examiner rejected claims 9 and 10 under 35 U.S.C. §103(a) as being unpatentable over Abbott in view of Vanzini and further in view of Polansky. Appellants respectfully traverse.

Claims 9 and 10 depend from claim 1, and are therefore allowable for at least the same reasons.

5. Rejection of claim 19

The Examiner rejected claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Abbott in view of Vanzini and further in view of Willins. Appellants respectfully traverse.

Claim 19 depends from claim 17, and is therefore allowable for at least the same reasons.

6. Rejection of claims 22, 24, and 26

The Examiner rejected claims 22, 24, and 26 under 35 U.S.C. § 103(a) as being unpatentable over Abbott in view of Vanzini and further in view of Terasaki. Appellants respectfully traverse.

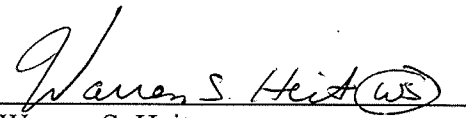
Claims 22, 24, and 26 depend from one of claims 1, 11, and 17, and are therefore allowable for at least the same reasons.

CONCLUSION

For the foregoing reasons, Appellants respectfully submit that the pending claims are not obvious in view of the cited references and are in condition for allowance.

Respectfully submitted,

Dated: August 29, 2008


Warren S. Heit
Reg. No. 36,828
Customer No. 007470
WHITE & CASE LLP
(650) 213-0321

APPENDIX A: CLAIMS APPENDIX

1. A unitary portable biometrics-based access control device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to a restricted resource, the device comprising:

a housing;

a microprocessor housed within the housing;

a non-volatile memory coupled to the microprocessor and capable of storing user data and having a minimum of 8 MB of capacity;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket; and

a biometrics-based authentication module coupled to and controlled by the

microprocessor, at least a portion of the biometrics-based authentication module being housed within the housing, wherein said biometrics-based authentication module is configured to grant access to the restricted resource provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise; and further wherein

said biometrics-based authentication module is configured to grant access to the user data stored in the non-volatile memory provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the user data stored in the non-volatile memory is denied to the user otherwise.

2. The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.
3. The portable device as recited in Claim 1 wherein the biometrics-based authentication module is an iris scan authentication module.
4. The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the housing.
5. The portable device as recited in Claim 1 further comprising a non-volatile memory capable of storing biometrics information usable for authentication.
6. The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.
7. The portable device as recited in Claim 1 wherein the restricted resource comprises a host computer.
8. The portable device as recited in Claim 1 wherein the restricted resource comprises a host computer.
9. The portable device as recited in Claim 1 wherein the restricted resource is a real estate premises that imposes access restrictions.

10. The portable device as recited in Claim 1 wherein the restricted resource is an operable machinery, the safe operation of which requires training.

11. A biometrics-based access control system for controlling access to a restricted resource, comprising:

a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource and which includes

a housing;

a non-volatile memory housed within the housing and having a minimum of 8 MB of capacity;

a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket; and

a biometrics-based authentication module coupled to the non-volatile memory,

wherein the biometrics-based authentication module is configured to (1) capture a first

biometrics marker, (2) store the first biometrics marker in the non-volatile

memory; (3) capture a second biometrics marker; and (4) determine whether the

second biometrics marker can be authenticated against the first biometrics marker,

and wherein access to the restricted resource is granted upon a determination of

successful authentication and wherein access to the restricted resource is denied

otherwise.

12. The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module is a fingerprint authentication module.

13. The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module is an iris scan authentication module.
14. The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module comprises a biometrics sensor which is structurally integrated with the portable device in a unitary construction, the biometrics sensor being disposed on one surface of the housing of the portable device.
15. The biometrics-based access control system as recited in Claim 11 wherein the non-volatile memory of the portable device comprises flash memory.
16. The biometrics-based access control system as recited in Claim 11 wherein a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.
17. A biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, the method comprising the steps of:
- (a) directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted resource, wherein the portable device includes a housing; a memory having a minimum of 8 MB of capacity; a biometrics sensor; and a USB plug integrated into the housing without an

intervening cable and capable of coupling the portable device directly to the USB socket;

- (b) obtaining a first biometrics marker from a user with the biometrics sensor of the portable device;
- (c) retrieving a registered biometrics marker from the memory of the portable device, the registered biometrics marker having been stored therein during a registration process;
- (d) comparing the first biometrics marker against the registered biometrics marker; and
- (e) granting the user access to the restricted resource provided that a match is identified in said step (d).

18. The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. The biometrics-based access control method as recited in Claim 17 further comprising the step of denying the user access to the restricted resource provided that a match is not identified in said step (d).

21. The biometrics-based access control method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (d).

22. The portable device as recited in Claim 1 wherein the non-volatile memory has a maximum of 512 MB of capacity.

23. The portable device as recited in Claim 1 wherein the non-volatile memory has capacity sufficient to serve as a mass-storage device.

24. The portable device as recited in Claim 11 wherein the non-volatile memory has a maximum of 512 MB of capacity.

25. The portable device as recited in Claim 11 wherein the non-volatile memory has capacity sufficient to serve as a mass-storage device.

26. The portable device as recited in Claim 17 wherein the memory has a maximum of 512 MB of capacity.

27. The portable device as recited in Claim 17 wherein the memory has capacity sufficient to serve as a mass-storage device.

APPENDIX B: EVIDENCE APPENDIX

NONE

APPENDIX C: RELATED PROCEEDINGS APPENDIX

NONE